

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application: 2002年10月10日

出願番号

Application Number: 特願2002-297550

[ ST.10/C ]:

[ JP2002-297550 ]

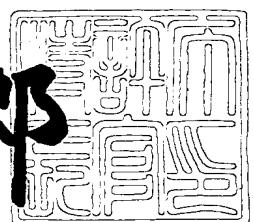
出願人

Applicant(s): 株式会社東芝

2003年 1月24日

特許庁長官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3001324

【書類名】 特許願  
【整理番号】 A000203876  
【提出日】 平成14年10月10日  
【あて先】 特許庁長官 殿  
【国際特許分類】 H04L 12/00  
G06F 12/00  
【発明の名称】 ネットワークシステム、情報処理装置、中継器およびネットワークシステムの構築方法  
【請求項の数】 16  
【発明者】  
【住所又は居所】 東京都青梅市末広町2丁目9番地 株式会社東芝青梅事業所内  
【氏名】 武田 淳  
【特許出願人】  
【識別番号】 000003078  
【氏名又は名称】 株式会社 東芝  
【代理人】  
【識別番号】 100058479  
【弁理士】  
【氏名又は名称】 鈴江 武彦  
【電話番号】 03-3502-3181  
【選任した代理人】  
【識別番号】 100084618  
【弁理士】  
【氏名又は名称】 村松 貞男  
【選任した代理人】  
【識別番号】 100068814  
【弁理士】  
【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークシステム、情報処理装置、中継器およびネットワークシステムの構築方法

【特許請求の範囲】

【請求項 1】 ネットワーク接続を行う端末と、  
前記端末の接続要求に際して認証を行うサーバと、  
前記端末からの認証要求を受け付け、当該要求受付時の情報をもとに前記端末  
の認証を行うサーバを特定し、前記要求を行った端末を前記特定したサーバに接  
続する処理装置と  
を具備したことを特徴とするネットワークシステム。

【請求項 2】 前記端末の認証を行うサーバは、ドメイン若しくはそれに類  
するネットワーク環境毎に設けられ、前記端末は、ドメイン若しくはそれに類す  
るネットワーク環境に特定されることなく設けられる請求項 1 記載のネットワー  
クシステム。

【請求項 3】 前記処理装置は、前記端末から前記要求を受け付けたとき、  
当該要求受付時の情報をもとに要求元の端末が所属するドメイン若しくはそれに  
類するネットワーク環境を認識し、自己の所属するドメイン若しくはそれに類す  
るネットワーク環境に所属するとき、前記サーバを特定する処理および前記接続  
の処理を実行する請求項 1 記載のネットワークシステム。

【請求項 4】 前記処理装置と前記端末は、無線 LAN により接続される請  
求項 1 記載のネットワークシステム。

【請求項 5】 ネットワーク接続を行う端末装置から認証要求を受け付ける  
手段と、

前記受け付けた要求をもとに当該要求を行った端末装置のアクセス資格の有無  
を検証する装置を特定する手段と、

前記要求を行った端末装置を前記特定した装置に接続する手段と  
を具備したことを特徴とする情報処理装置。

【請求項 6】 前記要求を行った端末装置のアクセス資格の有無を検証する  
装置を特定する手段は、前記要求受付時の情報をもとに前記端末装置の識別名を

取得し、当該識別名を用いたマッチングにより、前記端末装置が所属するドメイン若しくはそれに類するネットワーク環境を認識し、その認識結果をもとに前記要求を行った端末装置のアクセス資格の有無を検証する装置を特定することを特徴とする請求項5記載の情報処理装置。

【請求項7】 端末の接続要求に際して認証を行うサーバを具備したネットワークシステムに設けられる中継器であって、

端末からの認証要求をもとに当該要求を行った端末の認証を行うサーバを特定する手段と、

前記要求を行った端末を前記特定したサーバに接続する手段とを具備したことを特徴とする中継器。

【請求項8】 前記サーバを特定する手段は、ネットワーク接続可能な複数のドメイン若しくはそれに類するネットワーク環境と、その各ドメイン若しくはそれに類するネットワーク環境に置かれた認証を行うサーバとを対応付けて管理するテーブルを有し、前記要求の受付時に、前記端末より取得した情報と前記テーブルとを用いて、前記要求を行った端末の認証を行うサーバを特定することを特徴とする請求項7記載の中継器。

【請求項9】 前記端末との間で、IEEE 802.1Xの定義に従い、前記認証の手続きを行うことを特徴とする請求項7記載の中継器。

【請求項10】 前記端末との間で、EAPによる認証プロトコルを用いて前記認証の手続きを行うことを特徴とする請求項7記載の中継器。

【請求項11】 ネットワーク接続に際して認証を必要とするサプライカントと、

前記サプライカントの認証要求に際して認証を行うオーセンティケーションサーバと、

前記サプライカントから前記要求を受け付けて当該端末の認証を行うオーセンティケーションサーバを特定し、前記要求を行ったサプライカントを前記特定したオーセンティケーションサーバに接続するオーセンティケータとを具備したことを特徴とするネットワークシステム。

【請求項12】 前記オーセンティケータは、ネットワーク接続可能な複数

のドメイン若しくはそれに類するネットワーク環境に置かれたオーセンティケーションサーバ各々をその所属するドメイン若しくはそれに類するネットワーク環境とともに管理するテーブルを有して、前記サブリカントからの前記要求受付時に、当該サブリカントの識別情報を取得し、前記テーブルに設定されているドメイン若しくはそれに類するネットワーク環境の情報と前記取得した識別情報とのパターンマッチングにより前記端末の認証を行うオーセンティケーションサーバを特定する請求項11記載のネットワークシステム。

【請求項13】 前記オーセンティケータは、IEEE 802.1Xの定義に従い、前記サブリカントとの間で前記認証の手続きを行うことを特徴とする請求項11記載のネットワークシステム。

【請求項14】 前記オーセンティケータは、EAPによる認証プロトコルを用いて前記サブリカントとの間で前記認証の手続きを行うことを特徴とする請求項11記載のネットワークシステム。

【請求項15】 ネットワーク接続を行う端末と、前記端末からの要求に従い前記端末をネットワークに接続する中継装置と、前記端末の接続要求に際して認証を行うサーバとを具備したネットワークシステムの構築方法に於いて、

前記中継装置に、

前記端末からの認証要求を受け付け、当該要求受付時の情報をもとに前記端末の認証を行うサーバを特定する手段と、

前記要求を行った端末を前記特定したサーバに接続する手段とを備えて、

前記端末が自己の認証を行うサーバとは異なるネットワーク環境下に於いても自己の認証を行うサーバとの間で認証手続きを行うことができるようにしたこととを特徴とするネットワークシステムの構築方法。

【請求項16】 前記端末の認証を行うサーバを特定する手段は、ネットワーク接続可能な複数のドメイン若しくはそれに類するネットワーク環境と、その各ドメイン若しくはそれに類するネットワーク環境に置かれた認証を行うサーバとを対応付けて管理するテーブルを有し、前記要求の受付時に、前記端末より取得した情報と前記テーブルとを用いて、前記要求を行った端末の認証を行うサーバを特定することを特徴とする請求項15記載のネットワークシステムの構築方

法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、高度の認証手続きを必要とするネットワーク環境に適用される、ネットワークシステム、情報処理装置、中継器およびネットワークシステムの構築方法に関する。

【0002】

【従来の技術】

ネットワークへのアクセスに際して十分なセキュリティを確保する際、ユーザ認証のための装置が用いられる。代表的なユーザ認証装置として、RADIUSサーバが知られている（非特許文献1参照）。

【0003】

IEEE 802.1Xは、ポート単位でアクセスを制御するための規格である（非特許文献2参照）。具体的には、ネットワークに参加しようとする機器（ポートに接続した機器）に対して、認証処理をおこなう。そして、認証に成功した機器だけをネットワークに参加（ポートを開く）させる。

【0004】

ここで言うポートとは、イーサネット LANケーブルのような物理的なポートだけではなく、論理的なものも含まれる。たとえば、無線 LAN ネットワークの場合、ステーション（STA）とアクセスポイント（AP）間の接続が確立したとき（アソシエーションが確立したとき）、ステーション（STA）がポートに接続したとみなすことができる（図1に示すSTA、AP参照）。

【0005】

IEEE 802.1Xでは、以下の3つの構成単位（コンポーネント）が定義されている。

【0006】

（1）. サプリカント（Supplicant）

；認証されるコンポーネント。

## 【0007】

(2). オーセンティケータ (A u t h e n t i c a t o r)  
; サプリカント (S u p p l i c a n t) のアクセスを制御するコンポーネント。  
。ポートの開閉をおこなう。

## 【0008】

(3). オーセンティケーションサーバ (A u t h e n t i c a t i o n S e r v e r)  
; サプリカント (S u p p l i c a n t) の認証を行うコンポーネント。

## 【0009】

しかしながら、I E E E 8 0 2. 1 Xでは、特にオーセンティケータから、  
オーセンティケーションサーバへの通信について細かい規定がない。したがって  
、従来の技術に於いては、オーセンティケータは、あらかじめ指定していた（複  
数の）オーセンティケーションサーバに対して、固定的に通信を行っていた。こ  
れは、オーセンティケーションサーバが、すべてのサプリカントの認証を請け負  
うことを前提としている。

## 【0010】

この従来の技術では、互いに独立している環境下のサプリカントを、互いのネ  
ットワークに参加できるように再設定したい場合に、非常にコストがかかるこ  
とがある。

## 【0011】

たとえば、図7に示すように、オーセンティケーションサーバを各々にもつド  
メインAとドメインBのネットワーク環境が存在するものとする。この環境で、  
ドメインBに属するサプリカント (B) が、ドメインAのネットワークに参加し  
たり、逆に、ドメインAに属するサプリカント (A) が、ドメインBのネットワー  
ークに参加できるように環境を構築するには、第1の方法として、新たな一つの  
ドメイン (ドメインC) に纏め直すか、あるいは、第2の方法として、それぞれ  
のオーセンティケーションサーバが協調して、認証を請け負うように環境を構築  
する必要がある。ここで、「オーセンティケーションサーバの協調」とは、たと  
えば、R A D I U S P r o x yのような機能も含んでいる。

【0012】

上記第1の方法については、新たなネットワーク環境を構築しなければならないことからコストがかかる。また、第2の方法は、ネットワークを構築する上で簡易であるが、かならずしも、すべてのオーセンティケーションサーバに協調できるような機能がついているわけではなく、システム構成上の不安定要因を含んでいる。

【0013】

このように、従来では、各々異なるドメイン下にある各サプライカントが、それぞれのドメインのオーセンティケータを通してネットワークに参加できるシステムを構築しようとした際、種々の問題があった。

【0014】

【非特許文献1】

認証サーバソフトウェア 株式会社アクセンス・テクノロジー <http://accense.com/fullflex>

【0015】

【非特許文献2】

IEEE規格書802.1x-2001「ポート依存型ネットワークアクセス制御」(Port-Based Network Access Control) (2001年6月14日)

【0016】

【発明が解決しようとする課題】

上述したように、従来では、複数の環境（たとえばドメイン）下にある各サプライカントが、それぞれの環境（ドメイン）のオーセンティケータを通してネットワークに参加できるシステムを構築しようとした際、種々の問題があった。

【0017】

本発明は上記実情に鑑みなされたもので、ネットワーク環境を異にする各端末が、それぞれ相互のネットワーク環境下でアクセスできるシステムを構築する際に、高度のユーザ認証機構を経済的に有利な構成で容易に構築することのできるネットワークシステム、情報処理装置、中継器およびネットワークシステムの構

築方法を提供することを目的とする。

【0018】

また、本発明は、ドメイン等のネットワーク環境の再構築や、オーセンティケーションサーバの協調をおこなうことなく、複数の環境下にあるサプリカントが、それぞれ相互の環境下でアクセスできるネットワークシステムを構築できる情報処理装置、および中継器を提供することを目的とする。

【0019】

【課題を解決するための手段】

本発明は、ネットワーク接続に際して認証を必要とする端末からの認証要求に對して、その要求を受け付けた中継機能をもつ処理が、上記要求受付時の情報を用いて、適切な認証用サーバを選別することを特徴とする。

【0020】

即ち、本発明は、ネットワーク接続を行う端末と、前記端末の接続要求に際して認証を行うサーバと、前記端末からの認証要求を受け付け、当該要求受付時の情報をもとに前記端末の認証を行うサーバを特定し、前記要求を行った端末を前記特定したサーバに接続する処理装置とを具備したネットワークシステムを特徴とする。

【0021】

また、本発明は、ネットワーク接続を行う端末装置から認証要求を受け付ける手段と、前記受け付けた要求をもとに当該要求を行った端末装置のアクセス資格の有無を検証する装置を特定する手段と、前記要求を行った端末装置を前記特定した装置に接続する手段とを具備した情報処理装置を特徴とする。

【0022】

また、本発明は、端末の接続要求に際して認証を行うサーバを具備したネットワークシステムに設けられる中継器に於いて、端末からの認証要求をもとに当該要求を行った端末の認証を行うサーバを特定する手段と、前記要求を行った端末を前記特定したサーバに接続する手段とを具備したことを特徴とする。

【0023】

また、本発明は、ネットワーク接続を行う端末と、前記端末からの要求に従い

前記端末をネットワークに接続する中継装置と、前記端末の接続要求に際して認証を行うサーバとを具備したネットワークシステムの構築方法に於いて、前記中継装置に、前記端末からの認証要求を受け付け、当該要求受付時の情報をもとに前記端末の認証を行うサーバを特定する手段と、前記要求を行った端末を前記特定したサーバに接続する手段とを備えて、前記端末が自己の認証を行うサーバとは異なるネットワーク環境下に於いても自己の認証を行うサーバとの間で認証手続きを行うことができるようとしたことを特徴とする。

#### 【0024】

上記したような本発明の機能を備えることにより、ドメイン等のネットワーク環境を異にする各端末が、それぞれ相互のネットワーク環境下でアクセスできるシステムを構築する際に、高度のユーザ認証機構を経済的に有利な構成で容易に構築することができる。たとえば、IEEE 802.1Xの定義に従えば、サブリカントからの認証要求に対して、その要求を受け付けたオーセンティケータが、ネットワーク接続可能なドメイン等のネットワーク環境それぞれに置かれたオーセンティケーションサーバの中から、適切な（上記要求を出したサブリカントの認証を行う）オーセンティケーションサーバを選別することが可能となる。この機能により、複数のドメイン等のネットワーク環境下にあるサブリカントが、ドメインの再構築や、オーセンティケーションサーバの協調をおこなうことなく、ネットワーク接続を行う任意のドメイン等の環境下に於いて、そこに存在するオーセンティケータを通して、ネットワークに参加することができる。即ち、サブリカントは自己の所属するドメイン等の環境だけでなく、他の環境下にあるオーセンティケータとのアクセスで、自己の認証を行うオーセンティケーションサーバに対して認証を要求でき、その環境下でネットワーク接続を行うことができる。

#### 【0025】

##### 【発明の実施の形態】

以下、図面を参照して本発明の実施形態を説明する。

#### 【0026】

図1は本発明の実施形態に於けるシステムの構成を示すブロック図であり、こ

こでは、ドメインAの各コンポーネント（20A, 30A, 40A）がIP網10を介してドメインBの各コンポーネント（20B, 30B, 40B）にネットワーク接続された例を示している。

#### 【0027】

ドメインAには、オーセンティケーションサーバ（Authentication Server）となるRADIUSサーバ20（A）、およびオーセンティケータ（Authenticator）となるアクセスポイント（AP）30（A）が設けられる。更に、サプリカント（Supplicant）となるステーション（STA）40（A）が設けられる。

#### 【0028】

ドメインBには、オーセンティケーションサーバ（Authentication Server）となるRADIUSサーバ20（B）、およびオーセンティケータ（Authenticator）となるアクセスポイント（AP）30（B）が設けられる。更に、サプリカント（Supplicant）となるステーション（STA）40（B）が設けられる。尚、ここでは、説明を簡素にするため、各ドメインに於いて各コンポーネントをそれぞれ1台ずつ示している。また、上記各ドメインに設けられたステーション（STA）40（A），40（B）は、それぞれ汎用のパーソナルコンピュータを用いて実現され、各アクセスポイント（AP）30（A），30（B）と、ステーション（STA）40（A），40（B）との間は、それぞれ無線LANにより接続されるものとする。

#### 【0029】

上記各アクセスポイント（AP）30（A），30（B）には、それぞれ図2に示すようなルールテーブル（RT）31が設けられる。

#### 【0030】

このルールテーブル（RT）31は、各ステーション（STA）40（A），40（B）からの認証要求に対して、そのステーションの認証を行うRADIUSサーバを特定する際に用いられるもので、図2に示すように、ネットワーク接続が可能な各ドメインに設けられたRADIUSサーバ20（A），20（B）の情報（RADIUS情報）と、その各RADIUSサーバ20（A），20（B）が所属するドメインを特定できる比較文字列（条件パターン）とが対応付け

て設定され登録されている。

【0031】

上記ルールテーブル（R T）31上の比較文字列（条件パターン）は、認証手続きの際にステーション（S T A）40（A），40（B）から送られてくる、E A P - R e s p o n s e / I d e n t i t y（この実施形態ではサブリカント識別情報と称す）とのパターンマッチングの際に参照されるもので、その具体的なパターンマッチングについては図5を参照して後述する。

【0032】

図3は上記ルールテーブル（R T）31を用いたアクセスポイント（A P）30（A），30（B）の処理手順を示すフローチャートであり、ステーション（S T A）40（A／B）から認証要求を受け付けた際に実行される。

【0033】

図4は本発明の動作概念を示したもので、ここではI E E E 802.1Xの定義に従うコンポーネントを対象に、ドメインA，B間に於ける認証手続のルートを例に示している。

【0034】

図5は、上記実施形態に於いて、上記各アクセスポイント（A P）30（A），30（B）がステーション（S T A）40（A／B）から認証要求を受け付けた際に実行される上記ルールテーブル（R T）31を用いたパターンマッチングの動作を説明するためのサブリカント識別情報（E A P - R e s p o n s e / I d e n t i t y）の一例を示したもので、ここではドメイン名を含んだ形式の記載を例に示している。

【0035】

図6は上記認証時の処理およびデータの流れを簡単に示したもので、ここではI E E E 802.1Xの定義に従うコンポーネントを対象に示している。また、ここではオーセンティケーションサーバ（A u t h e n t i c a t i o n S e r v e r）にR A D I U Sサーバを使用しているが、これに限るものではない。

【0036】

図中の（3）と（4）との間で、図3に示す、認証要求に従うR A D I U Sサ

ーバ20（A／B）を特定する処理が実行される。

【0037】

ここで、上記図1乃至図6を参照して本発明の実施形態に於ける動作を説明する。

【0038】

本発明の実施形態を説明するに際して、認証要求時に於けるデータの流れを図6を参照して説明する。ここでは認証が成功した例を示している。

【0039】

(1) E A P O L - S t a r t

サプライカント（Supplicant）がオーセンティケータ（Authenticator）に認証の開始を要求する。

【0040】

(2) E A P - R e q u e s t / I d e n t i t y

オーセンティケータ（Authenticator）がサプライカント（Supplicant）にサプライカント識別情報（E A P - R e s p o n s e / I d e n t i t y）を要求する。

【0041】

(3) E A P - R e s p o n s e / I d e n t i t y

サプライカント（Supplicant）がオーセンティケータ（Authenticator）にサプライカント識別情報（E A P - R e s p o n s e / I d e n t i t y）を返答する。

【0042】

(4) A c c e s s   R e q u e s t

オーセンティケータ（Authenticator）がオーセンティケーションサーバ（Authentication Server）にサプライカント（Supplicant）の認証を要求する。上記（3）と（4）の間に於いて、図3に示す処理が行われる。

【0043】

(5) A c c e s s   C h a l l e n g e

オーセンティケーションサーバ（Authentication Server）からオーセンティケータ（Authenticator）に、認証のためのチャレンジが返される。

【0044】

## (6) EAP Authentication Process

サプリカント (Supplicant) とオーセンティケーションサーバ (Authentication Server) との間で認証処理が行われる。本来、細かいやりとりを行っているが、ここでは省略する。

【0045】

## (7) Access Accept

オーセンティケーションサーバ (Authentication Server) がオーセンティケータ (Authenticator) に、サプリカント (Supplicant) を認証した旨を通知する。認証に失敗した場合は、Access Rejectが返る。

【0046】

## (8) EAP-Success

オーセンティケータ (Authenticator) がサプリカント (Supplicant) に、認証が成功した旨を通知する。

【0047】

ここで、本発明の基本的な動作概念を図4を参照して説明する。

【0048】

ドメインAに於いてサプリカント (Supplicant) のアクセスを行うオーセンティケータ (Authenticator) Aは、サプリカント (Supplicant) Bが（例えば無線LANを介して）ポートに接続してきた際、サプリカント (Supplicant) Bの認証を行うオーセンティケーションサーバ (Authentication Server) Bを選択して、認証処理を開始する。この際、オーセンティケータ (Authenticator) Aは、ポートに接続してきたサプリカント (Supplicant) が、どのドメインに属しているのか判別する必要がある。この判別の際に、サプリカント (Supplicant) から受けた、上記図6（3）に示されるサプリカント識別情報（EAP-Response/Identity）を利用する。

【0049】

このサプリカント識別情報（EAP-Response/Identity）には、サプリカント (Supplicant) の識別名が記載されている。この記載内容については、特に規定されていないが、たとえば、図5に示すようなドメイン名を含んだ形式で記載

される。

【0050】

図6(3)に於いて、サプライカント識別情報(EAP-Response/Identity)が、サプライカント(Suppliant)から送信されるので、オーセンティケータ(Authenticator)は、そのサプライカント識別情報(EAP-Response/Identity)から、そのサプライカント(Suppliant)が属しているドメインを判別し、そのドメインに属している適切なオーセンティケーションサーバ(Authentication Server)に対して上記図6(4)以降の通信を開始する。

【0051】

次に、図1に示すネットワークシステムに於ける認証処理について、図1乃至図3を参照して説明する。

【0052】

図1に於いて、RADIUSサーバ20(A)は、ドメインAに属する各ステーション(STA)40(A)の認証を行う。RADIUSサーバ20(B)はドメインBに属する各ステーション(STA)40(B)の認証を行う。

【0053】

アクセスポイント(AP)30(A)は、ドメインAに属するステーション(STA)40(A)のアクセスを制御する。アクセスポイント(AP)30(B)は、ドメインBに属するステーション(STA)40(B)のアクセスを制御する。

【0054】

ステーション(STA)40(A), 40(B)は、上記各アクセスポイント(AP)30(A), 30(B)との間で、例えば無線LANを介して接続される。尚、図1では、ステーション(STA)40(B)が、例えば携帯型のパーソナルコンピュータを用いて構成され、本来、所属するドメインBのアクセスポイント(AP)30(B)から切り離されて、ドメインAのアクセスポイント(AP)30(A)に接続要求を行う場合を例示している。

【0055】

この際、アクセスポイント（AP）30（A）は、ステーション（STA）40（B）から接続要求に際して、認証要求（図6（1）に示すEAPOL-Start；認証の開始要求）を受けることにより、上記した図6に示す認証のためのデータ授受が開始される。この図6に示す（3）と（4）の間に於いて、図3に示す、認証要求に従うRADiUSサーバ20（A/B）を特定する処理が実行される。

#### 【0056】

この処理は、図2に示すルールテーブル（RT）31を参照して行われる。

#### 【0057】

アクセスポイント（AP）30（A）は、ステーション（STA）40（B）から上記認証の開始要求を受けると（図6（1）参照）、ステーション（STA）40（B）にサプリカント識別情報（EAP-Response/Identity）を要求する（図6（2）参照）。

#### 【0058】

この要求に従い、ステーション（STA）40（B）からサプリカント識別情報（EAP-Response/Identity）を取得すると、そのサプリカント識別情報（EAP-Response/Identity）に含まれる図5に示すような識別名の一部（例えばドメイン名）を用いて、図2に示すルールテーブル（RT）31とのパターンマッチングにより、ステーション（STA）40（B）の認証を行うRADiUSサーバ20（A/B）を検索する。即ち、認証要求を出したステーション（STA）40（B）と同じドメイン名若しくはそれに類する文字列構造をもつRADiUS情報を検索する（図3ステップS31, S32）。

#### 【0059】

ここで、ステーション（STA）40（B）と同じドメイン名若しくはそれに類する文字列構造をもつRADiUS情報が存在（パターンマッチ）すると、ルールテーブル（RT）31のパターンマッチした個所に記述されているIPアドレス、ポート番号等から認証要求先のRADiUSサーバ20（B）を決定し（図3ステップS33）、決定したRADiUSサーバ20（B）に図6（4）に示すAccess Requestを送付して認証を要求する。

## 【0060】

このような処理により、ドメインの再構築や、オーセンティケーションサーバ同士が協調して動作しなくても、ネットワーク環境を異にする各端末（ステーション）が、それぞれ相互のネットワーク環境下でアクセスできる。

## 【0061】

尚、本発明は、IEEE 802.1Xに限らず、EAP (Extensible Authentication Protocol) による認証プロトコルを採用し、かつ、端末と認証サーバの間に立って、中継をおこなうようなすべてのシステムに適用できる。たとえば、RAS (Remote Access Server) にも適用可能である。

## 【0062】

## 【発明の効果】

以上詳記したように、本発明によれば、ネットワーク環境を異にする各端末が、それぞれ相互のネットワーク環境下でアクセスできるシステムを構築する際に、高度のユーザ認証機構を経済的に有利な構成で容易に構築することができる。

## 【図面の簡単な説明】

## 【図1】

本発明の第1実施形態に於けるシステムの構成を示すブロック図。

## 【図2】

上記実施形態に於けるルールテーブル（RT）の構成例を示す図。

## 【図3】

上記実施形態に於けるルールテーブル（RT）を用いたアクセスポイントの処理手順を示すフローチャート。

## 【図4】

本発明の動作概念を示す図。

## 【図5】

上記実施形態に於けるルールテーブル（RT）を用いたパターンマッチングの動作を説明するためのサプリカント識別情報（EAP-Response/Identification）の一例を示す図。

## 【図6】

上記実施形態に於ける認証時の処理の流れを示す図。

【図7】

本発明で対象とするネットワーク環境の基本的な構成例を示す図。

【符号の説明】

1 0 … I P 網

2 0 (A) , 3 0 (B) … R A D I U S サーバ

3 0 (A) , 3 0 (B) … アクセスポイント (A P)

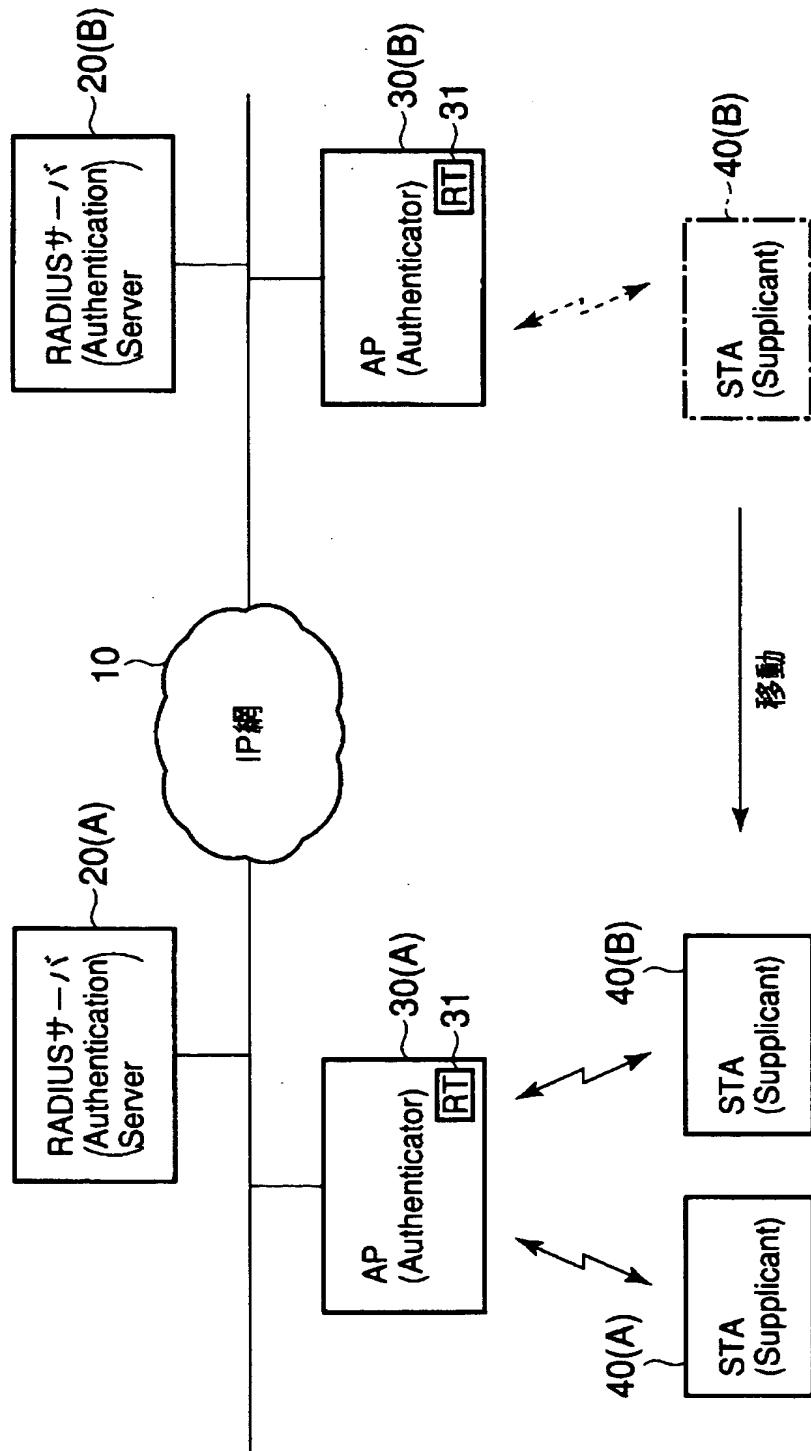
3 1 … ルールテーブル (R T)

4 0 (A) , 4 0 (B) … ステーション (S T A)

【書類名】

図面

【図1】



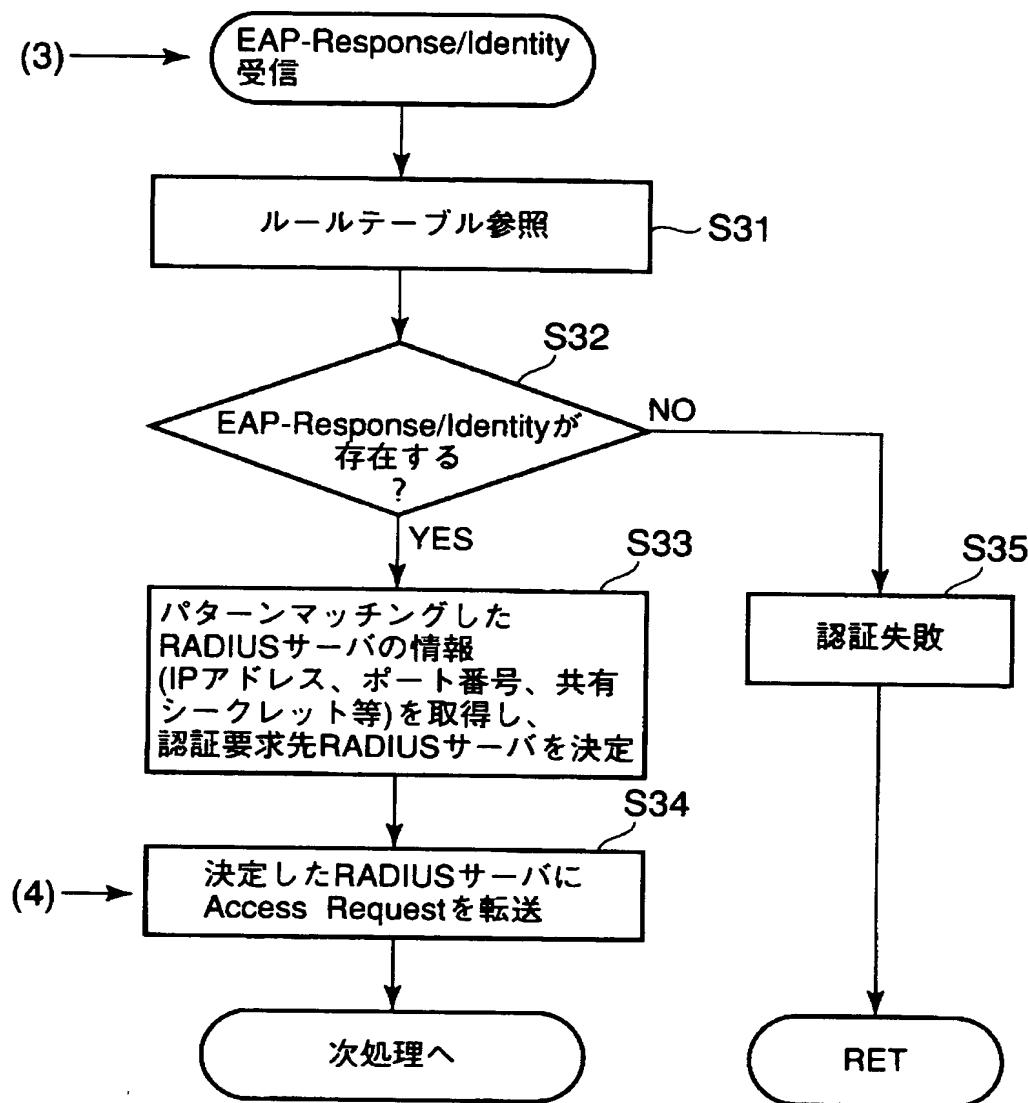
【図2】

ルールテーブル(RT)

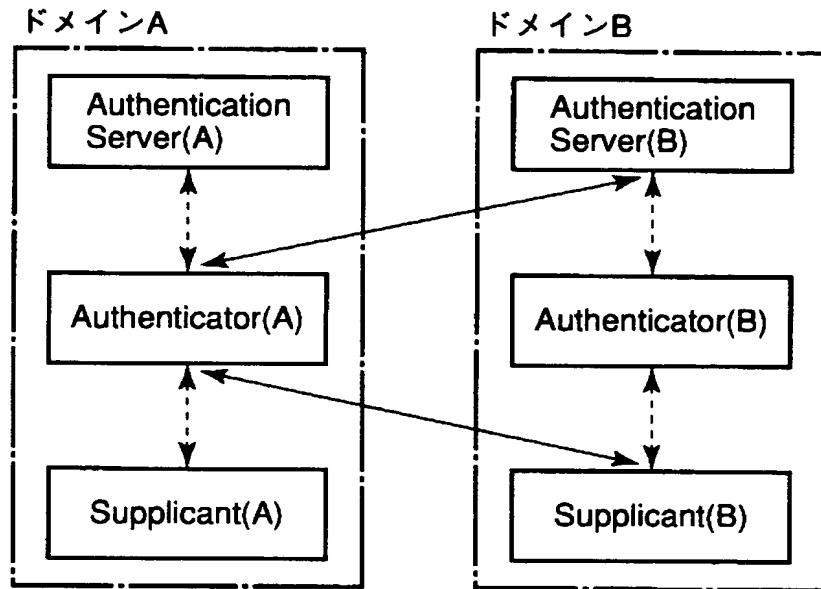
31

| EAP-Response/Identity<br>比較文字列(条件パターン) | RADIUS情報<br>(IPアドレス、ポート番号、<br>共有シークレット等) |
|--|--|
| DOMAIN-B¥*                             | RADIUS-B                                 |
| *@domain-a. .... .co.jp                | RADIUS-A                                 |
| ⋮                                      | ⋮  |

【図3】



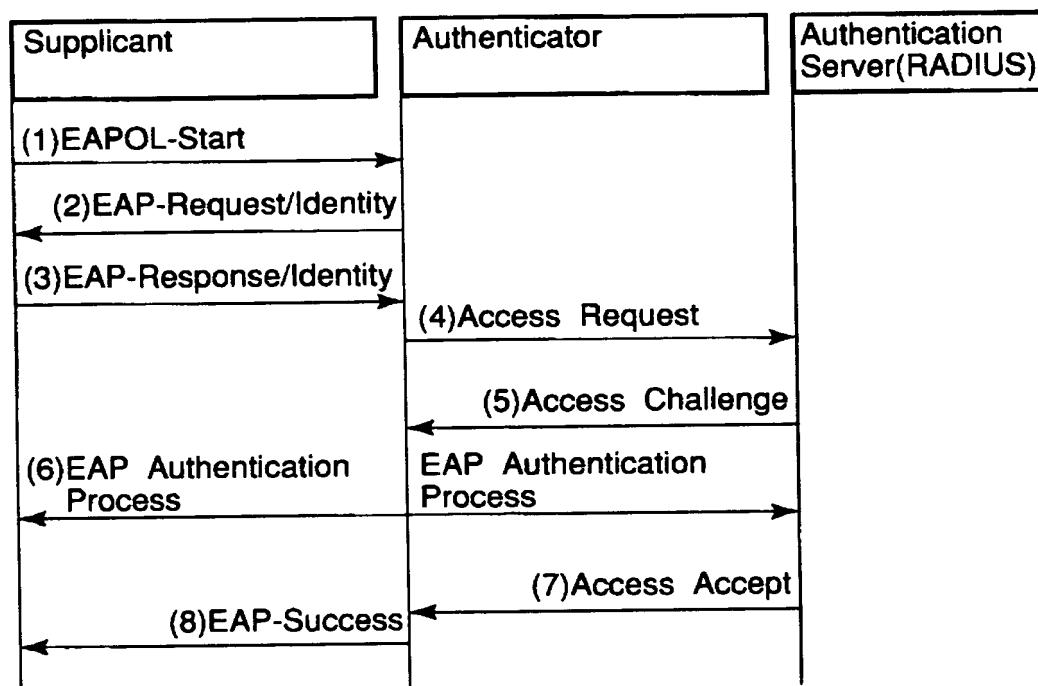
【図4】



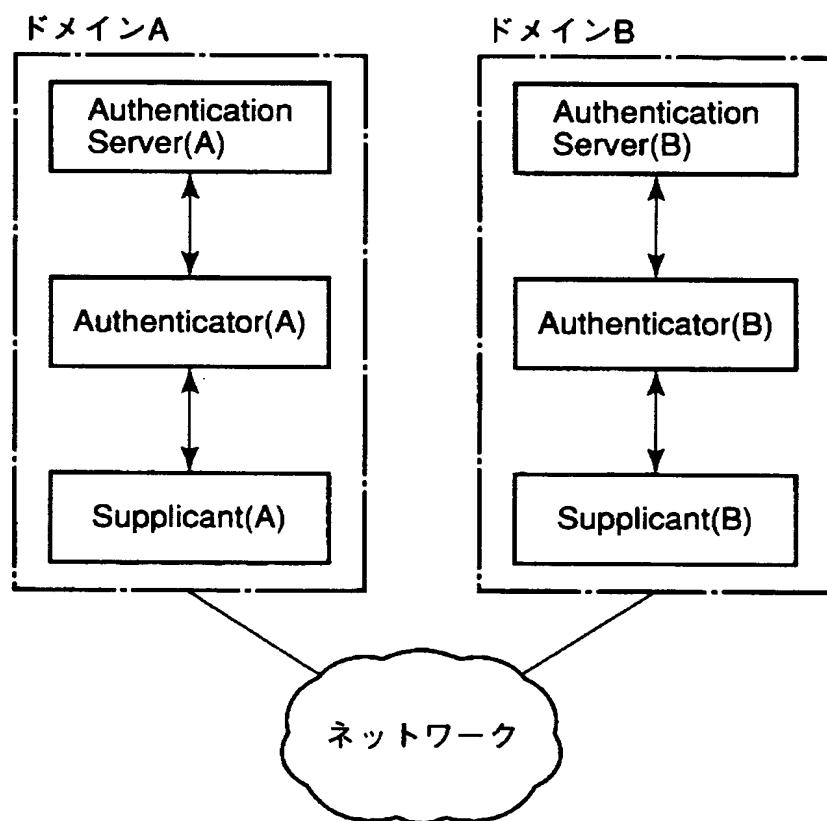
【図5】

|                      |   |
|----------------------|---|
| NETBIOS ドメイン名を使用した表現 | <ドメイン名>¥<ユーザ名>の形式で記載される<br>例: DOMAIN-A¥user01             |
| DNS ドメイン名を使用した表現     | <ユーザ名>@<ドメイン>の形式で記載される<br>例: user01@domain-a.tosxxx.co.jp |

【図6】



【図7】



【書類名】 要約書

【要約】

【課題】 本発明は、ドメイン等のネットワーク環境の再構築や、オーセンティケーションサーバの協調をおこなうことなく、複数の環境下にあるサプライカントが、それぞれ相互の環境下でアクセスできるネットワークシステム、中継装置、およびその構築方法を提供することを課題とする。

【解決手段】 アクセスポイント（A P）30（A）は、ステーション（S T A）40（B）から認証の開始要求を受けると、ステーション（S T A）40（B）からサプライカント識別情報（E A P - Response / Identity）を取得して、ルールテーブル（R T）31とのパターンマッチングにより、アクセスポイント（A P）30（B）の認証を行うR A D I U S サーバ20（A / B）を検索する。

【選択図】 図1

出願人履歴情報

識別番号 [000003078]

1. 変更年月日 2001年 7月 2日

[変更理由] 住所変更

住 所 東京都港区芝浦一丁目1番1号  
氏 名 株式会社東芝